

EPISEN

Ing3 2023-2024

Module SL

APPRENTISSAGE DE MODÈLES

Analyse *a posteriori* des systèmes d'informations.

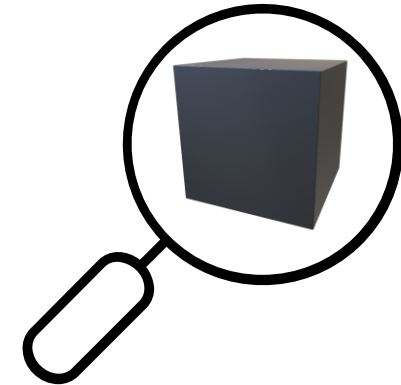
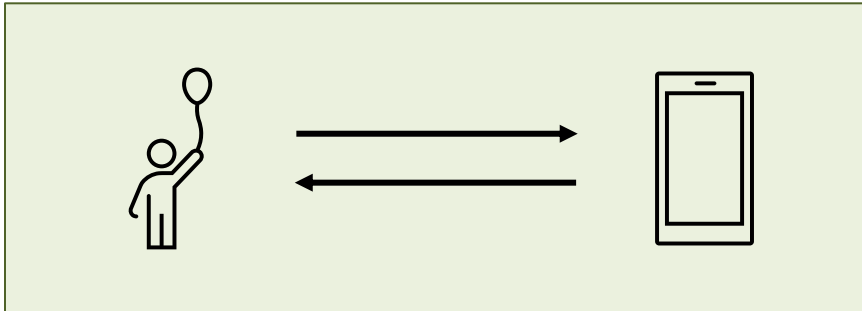
- Vérifier la conformité du système final par rapport à sa spécification.
- Détecter des erreurs introduites par les éléments hors de notre contrôle:
 - Compilateur/interpréteur/machine virtuelle,
 - Librairies externes,
 - APIs
 - ...
- Obtenir un modèle d'un système tiers, pour lequel on ne dispose pas de spécification appropriée.

Analyse « boîte noire »

Définition

Analyse d'un système par ses interactions avec son environnement, sans connaissance de sa structure interne.

Exemple



Analyse active ou passive

Analyse active

- Les techniques **actives** réalisent des expériences sur le système analysé.
- On a besoin d'une **interface** pour communiquer avec le système.
- Permet d'obtenir des modèles aussi précis qu'on le désire.

Analyse passive

- Les techniques **passives** utilisent des traces d'exécutions (journaux/logs) du système.
- Ces techniques ne nécessitent pas d'avoir accès au système.
- Analyse limitée aux comportements observés dans les journaux.

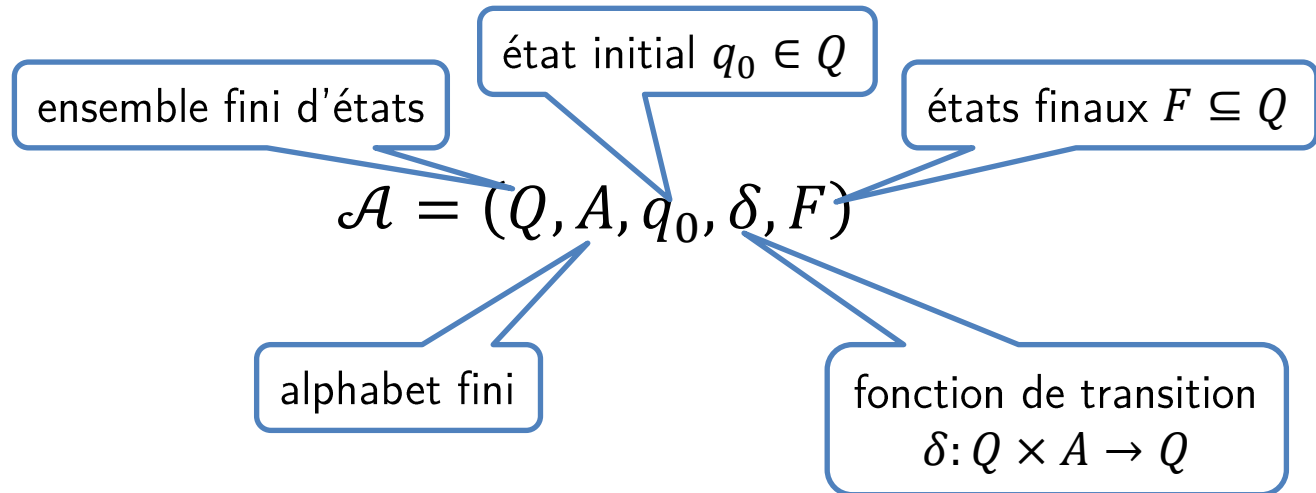
Plan du cours

1. Apprentissage d'automates finis
 1. Rappels sur les automates
 2. Enseignant idoine et L^*
2. Apprentissage de diagrammes états transitions
 1. Machines de Mealy
 2. L^* pour les machines de Mealy
3. Applications

1. Rappels sur les automates
2. Enseignant idoine et L^*

APPRENTISSAGE D'AUTOMATES FINIS

Automates à états finis



Définition

$$\delta^*: Q \times A^* \rightarrow Q$$

$$\delta^*(q, \varepsilon) := q$$

$$\delta^*(q, au) := \delta^*(\delta(q, a), u)$$

Définition

Langage reconnu par un automate :

$$[[\mathcal{A}]] := \{u \in A^* \mid \delta^*(q_0, u) \in F\}$$

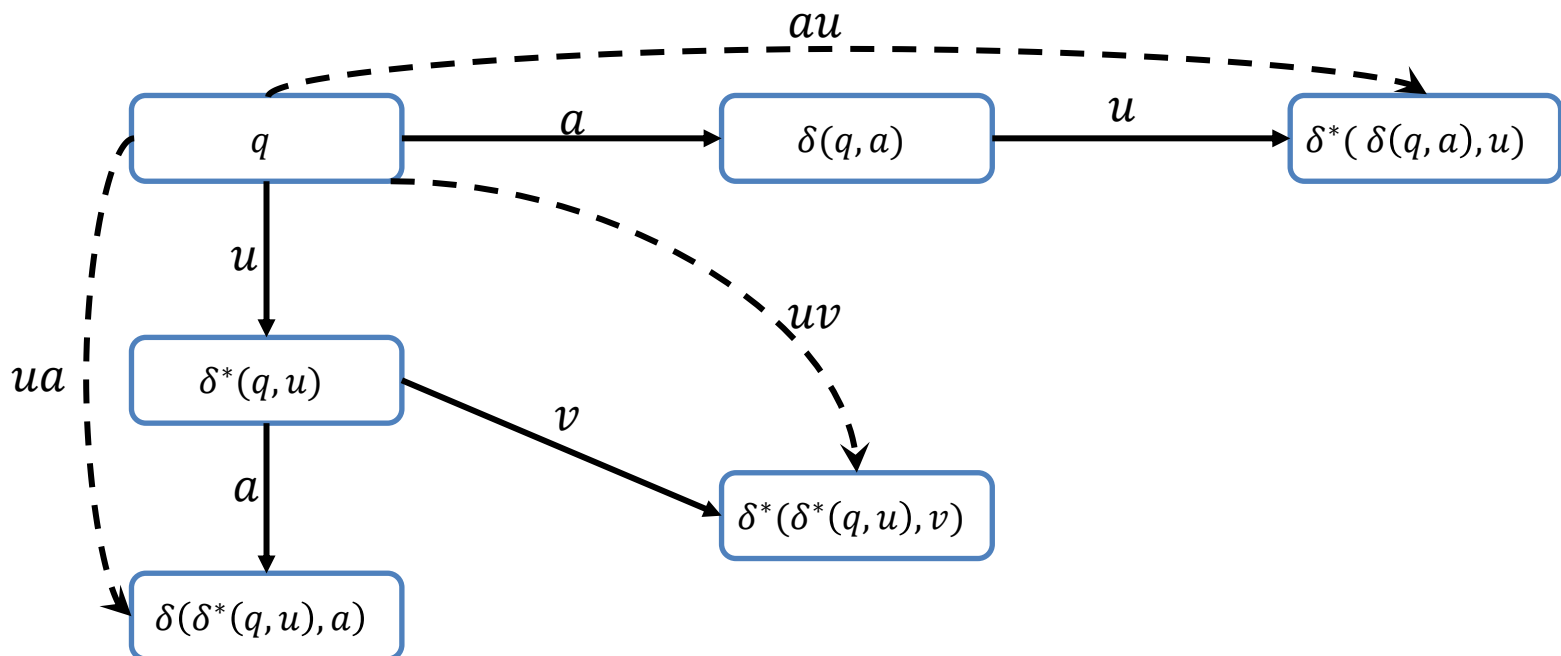
Remarque sur la fonction de transition

Soit $\mathcal{A} = (Q, A, q_0, \delta, F)$ un automate déterministe.

Propriété

Pour tout état $q \in Q$, tous mots $u, v \in A^*$ et toute lettre $a \in A$, on a :

- $\delta^*(q, au) = \delta^*(\delta(q, a), u)$
- $\delta^*(q, ua) = \delta(\delta^*(q, u), a)$
- $\delta^*(q, uv) = \delta^*(\delta^*(q, u), v)$



Automate minimal et théorème de Myhill-Nerode

Définition

Soit un langage $L \subseteq A^*$. La **congruence de Myhill-Nerode** associée à L est la relation \equiv_L sur A^* définie par:

$$u \equiv_L v \Leftrightarrow \forall w \in A^*, uw \in L \text{ ssi } vw \in L$$

L'index de \equiv_L est l'ensemble de ses classes d'équivalence, c'est-à-dire les ensembles de mots $[u]_L := \{v \in A^* \mid u \equiv_L v\} \subseteq A^*$.

L rationnel signifie qu'il existe un automate \mathcal{A} tel que $L = \llbracket \mathcal{A} \rrbracket$.

Théorème

L est rationnel si et seulement si \equiv_L est d'index fini.

Dans ce cas, tout automate minimal reconnaissant L est isomorphe à l'automate suivant:

- $Q := \{[u]_L \mid u \in A^*\}$
- $q_0 := [\varepsilon]_L$
- $\delta([u]_L, a) := [ua]_L$
- $F := \{[u]_L \mid u \in L\}$

Il est appelé **automate de Myhill-Nerode**.

Exemples de relation de MN

Langage des mots contenant un nombre pair de a

Notation : $|u|_a$ est le nombre d'occurrences de la lettre a dans le mot u .

Formellement : $|\varepsilon|_a := 0$

$|au|_a := 1 + |u|_a$

$|bu|_a := |u|_a$ si $a \neq b$

Exemples : $|abc|_a = 1$

$|baba|_a = 2$

$L_1 := \{u \in \{a, b\}^* \mid |u|_a \text{ est pair}\}.$

- $\varepsilon \equiv_{L_1} u$
 - $\Leftrightarrow (\forall w \in \{a, b\}^*, w \in L_1 \Leftrightarrow uw \in L_1)$
 - $\Leftrightarrow (\forall w \in \{a, b\}^*, |w|_a \text{ pair} \Leftrightarrow |uw|_a = |u|_a + |w|_a \text{ pair})$
 - $\Leftrightarrow |u|_a \text{ pair}$
- $a \equiv_{L_1} u$
 - $\Leftrightarrow (\forall w \in \{a, b\}^*, aw \in L_1 \Leftrightarrow uw \in L_1)$
 - $\Leftrightarrow (\forall w \in \{a, b\}^*, |aw|_a = 1 + |w|_a \text{ pair} \Leftrightarrow |uw|_a = |u|_a + |w|_a \text{ pair})$
 - $\Leftrightarrow |u|_a \text{ impair}$
- Comme tout mot a soit un nombre pair de a , soit un nombre impair de a , cela signifie que tout mot est soit équivalent au mot vide, soit équivalent au mot a .
Autrement dit:

$$\{a, b\}^* = [\varepsilon]_{L_1} \cup [a]_{L_1}$$

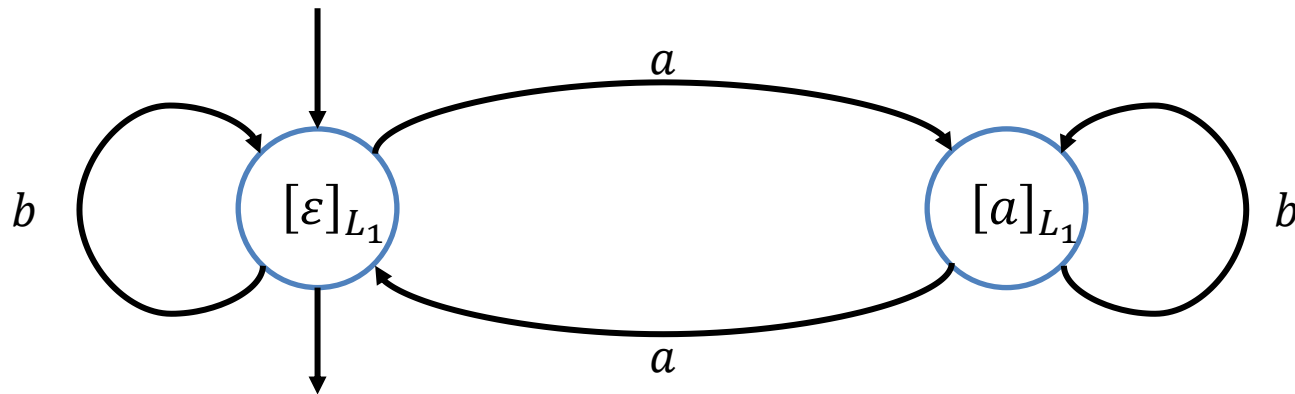
Exemples de relation de MN

Langage des mots contenant un nombre pair de a

$L_1 := \{u \in \{a, b\}^* \mid |u|_a \text{ est pair}\}.$

$$\boxed{\{a, b\}^* = [\varepsilon]_{L_1} \cup [a]_{L_1}}$$

On construit l'automate minimal:



Les transitions ont été calculées avec la formule $\delta([u]_L, a) := [ua]_L$, c'est-à-dire :

- $\delta([\varepsilon]_{L_1}, a) := [a]_{L_1}$
- $\delta([\varepsilon]_{L_1}, b) := [b]_{L_1} = [\varepsilon]_{L_1}$ car comme $|b|_a = 0$, on a $\varepsilon \equiv_{L_1} b$
- $\delta([a]_{L_1}, a) := [aa]_{L_1} = [\varepsilon]_{L_1}$ car comme $|aa|_a = 2$, on a $\varepsilon \equiv_{L_1} aa$
- $\delta([a]_{L_1}, b) := [ab]_{L_1} = [a]_{L_1}$ car comme $|ab|_a = 1$, on a $a \equiv_{L_1} ab$

Le seul état final est $[\varepsilon]_{L_1}$ car $\varepsilon \in L_1$ mais $a \notin L_1$.

Exemples de relation de MN

Langage des $a^n b^n$

Notation : u^n est le mot obtenu en concaténant n copies du mot u en séquence.

Formellement : $u^0 := \varepsilon$ $u^{n+1} := u u^n$

Exemples : $(abc)^2 = abcabc$ $a^4 := aaaa$

$L_2 := \{a^n b^n \mid n \in \mathbb{N}\}$.

Considérons la suite $(a^n)_{n \in \mathbb{N}}$.

Pour toute paire $n \neq m$, on peut montrer que $a^n \not\equiv_{L_2} a^m$. En effet, en choisissant le suffixe $w := b^n$, on obtient $a^n b^n \in L_2$ et $a^m b^n \notin L_2$.

En conséquence, il est impossible que deux éléments distincts de cette suite infinie appartiennent à la même classe d'équivalence.

On en déduit que la relation \equiv_{L_2} a un nombre infini de classes d'équivalence.

Autrement dit \equiv_{L_2} est **d'index infini**.

En vertu du théorème de Myhill-Nerode, cela signifie que L_2 n'est pas rationnel.

Principe des tiroirs

Intuition

Si on a plus de chaussettes que de tiroirs, et qu'on met toutes les chaussettes dans des tiroirs, alors il existe un tiroir contenant au moins deux chaussettes.

Formellement

Soient deux ensembles finis A et B tels que le cardinal (nombre d'éléments) de A est strictement plus grand que le cardinal de B , et une fonction $f: A \rightarrow B$. Alors il existe $a_1, a_2 \in A$ tels que $a_1 \neq a_2$ et $f(a_1) = f(a_2)$.

Les éléments de A sont les chaussettes, les éléments de B sont les tiroirs, et la fonction f associe à chaque chaussette le tiroir où elle est rangée.

Conséquence

Soient deux ensembles A et B tels que l'ensemble B est fini, et une fonction $f: A \rightarrow B$ telle que pour toute paire $a_1 \neq a_2 \in A$ d'éléments distincts de A on a $f(a_1) \neq f(a_2)$. Alors A est un ensemble fini, et $\#A \leq \#B$.

$\#A$: cardinal de A , c'est-à-dire le nombre d'éléments de A .
Par exemple $\#\{a, b, c\} = 3$, et $\#\emptyset = 0$.

Éléments de preuve du théorème de Myhill-Nerode

Soit L rationnel

Par définition, il existe un automate \mathcal{A} tel que $[[\mathcal{A}]] = L$.

On va montrer que \equiv_L a moins de classes d'équivalence que \mathcal{A} n'a d'états.

Soient u, v deux mots tels que $\delta^*(q_0, u) = \delta^*(q_0, v)$. Montrons que $u \equiv_L v$.

Soit un suffixe $w \in A^*$. Alors:

- $uw \in L \Leftrightarrow \delta^*(q_0, uw) \in F$ et $vw \in L \Leftrightarrow \delta^*(q_0, vw) \in F$
- $\delta^*(q_0, uw) = \delta^*(\delta^*(q_0, u), w) = \delta^*(\delta^*(q_0, v), w) = \delta^*(q_0, vw)$
- Par conséquent on obtient:

$$uw \in L \Leftrightarrow \delta^*(q_0, uw) \in F \Leftrightarrow \delta^*(q_0, vw) \in F \Leftrightarrow vw \in L,$$

et donc $u \equiv_L v$.

On définit une fonction $f: A^* \rightarrow Q$ telle que $f(u) := \delta^*(q_0, u)$. La propriété ci-dessus se réécrit donc : $f(u) = f(v) \Rightarrow u \equiv_L v$. Par contraposition, cela donne:

$$\boxed{u \not\equiv_L v \Rightarrow f(u) \neq f(v)}$$

On montre que \equiv_L est d'index fini:

Soit un ensemble $X \subseteq A^*$ de mots inéquivalents, c'est-à-dire tel que $\forall x \neq y \in X, x \not\equiv_L y$.

Cela implique que $\forall x \neq y \in X, f(x) \neq f(y)$.

Par le principe des tiroirs, et puisque Q est fini, on en déduit que X est fini, et a moins d'éléments que Q .

En particulier, si on choisit un ensemble de représentants de chaque classe d'équivalence de \equiv_L (un ensemble X d'éléments inéquivalents tel que pour tout mot u , il existe $x \in X$ tel que $u \equiv_L x$), alors on obtient que \equiv_L a moins de classes d'équivalence de $\#Q$.

Éléments de preuve du théorème de Myhill-Nerode

Soit L tel que \equiv_L est d'index fini

- On commence par montrer que l'automate de Myhill-Nerode est bien défini.

$\mathcal{A} := (\{[u]_L \mid u \in A^*\}, A, [\varepsilon]_L, \delta, \{[u]_L \mid u \in L\})$ où $\delta([u]_L, a) := [ua]_L$.

1. L'ensemble des états est fini, puisque \equiv_L est d'index fini.

2. La fonction de transition est bien définie:

Pour que δ soit bien définie comme fonction, il faut s'assurer que si $[u]_L = [v]_L$ alors $\delta([u]_L, a) = \delta([v]_L, a)$, c'est-à-dire $[ua]_L = [va]_L$. Autrement dit, on cherche à prouver que si $u \equiv_L v$, alors on a $ua \equiv_L va$.

Soit $w \in A^*$, on obtient: $uaw \in L$ ssi $u(aw) \in L$ ssi $v(aw) \in L$ ssi $vaw \in L$.

3. Les états finaux ne dépendent pas du choix des représentants:

Observons que $u \equiv_L v$ implique $u = u\varepsilon \in L \Leftrightarrow v = v\varepsilon \in L$. Par conséquent, on obtient:

$$[v]_L \in \{[u]_L \mid u \in L\} \Leftrightarrow \exists u \in L : v \equiv_L u \Leftrightarrow v \in L$$

- Ensuite, on vérifie que $\llbracket \mathcal{A} \rrbracket = L$.

Pour cela, on commence par montrer par induction sur u que $\delta^*([\varepsilon]_L, u) = [u]_L$:

$$\delta^*([\varepsilon]_L, \varepsilon) = [\varepsilon]_L \text{ et } \delta^*([\varepsilon]_L, ua) = \delta(\delta^*([\varepsilon]_L, u), a) = \delta([u]_L, a) = [ua]_L.$$

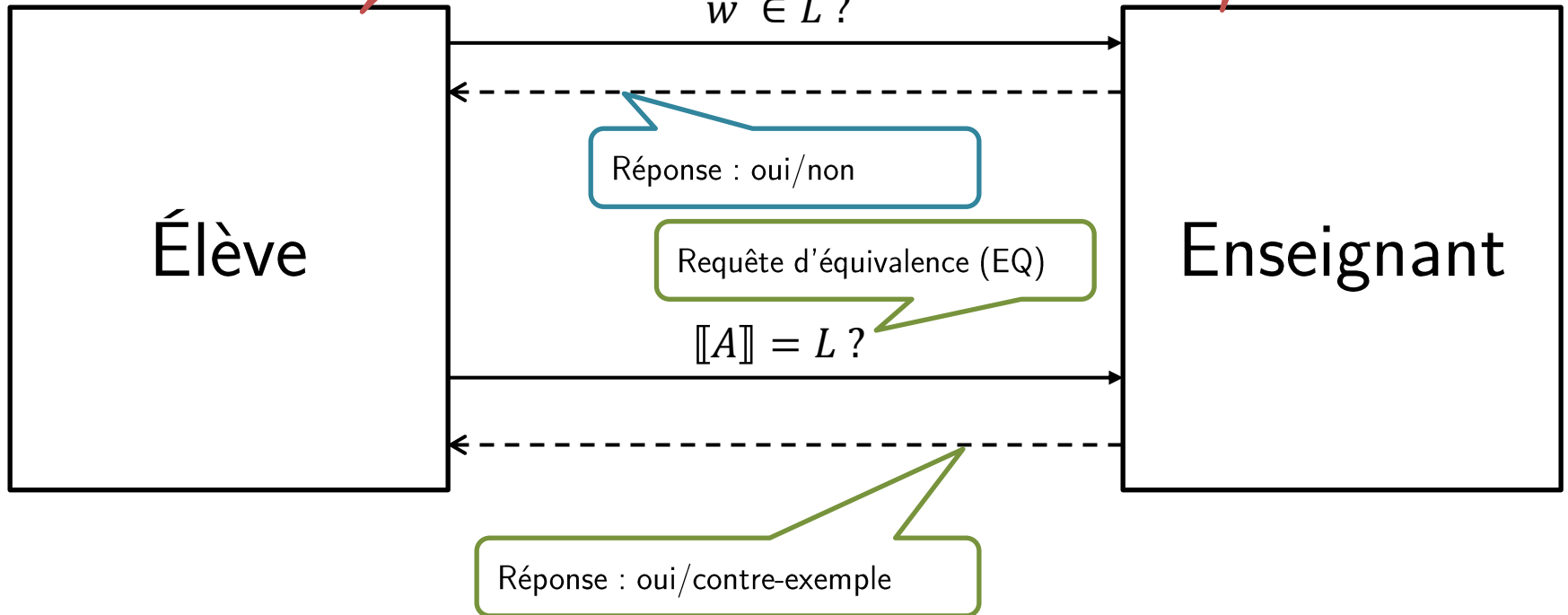
On peut conclure:

$$u \in \llbracket \mathcal{A} \rrbracket \Leftrightarrow \delta^*([\varepsilon]_L, u) \in \{[u]_L \mid u \in L\} \Leftrightarrow [u]_L \in \{[u]_L \mid u \in L\} \Leftrightarrow u \in L.$$



Dana Angluin

L'enseignant idoine



Algorithme L^*

1. On construit une table d'observation.
2. Tant que la table est « incomplète » (qu'elle ne permet pas de construire un automate), on l'étend grâce à des requêtes d'appartenance.
3. Lorsque cette table est « complète » (c'est-à-dire qu'elle correspond à un automate), on l'utilise pour générer un automate « hypothèse ».
4. On soumet cette hypothèse à l'enseignant via une requête d'équivalence.
 - a) Si l'enseignant fournit un contre exemple, on étend la table avec ce contre-exemple, et on reprend l'étape 2.
 - b) Si l'enseignant répond oui, on a gagné.

Table d'observation

Définition

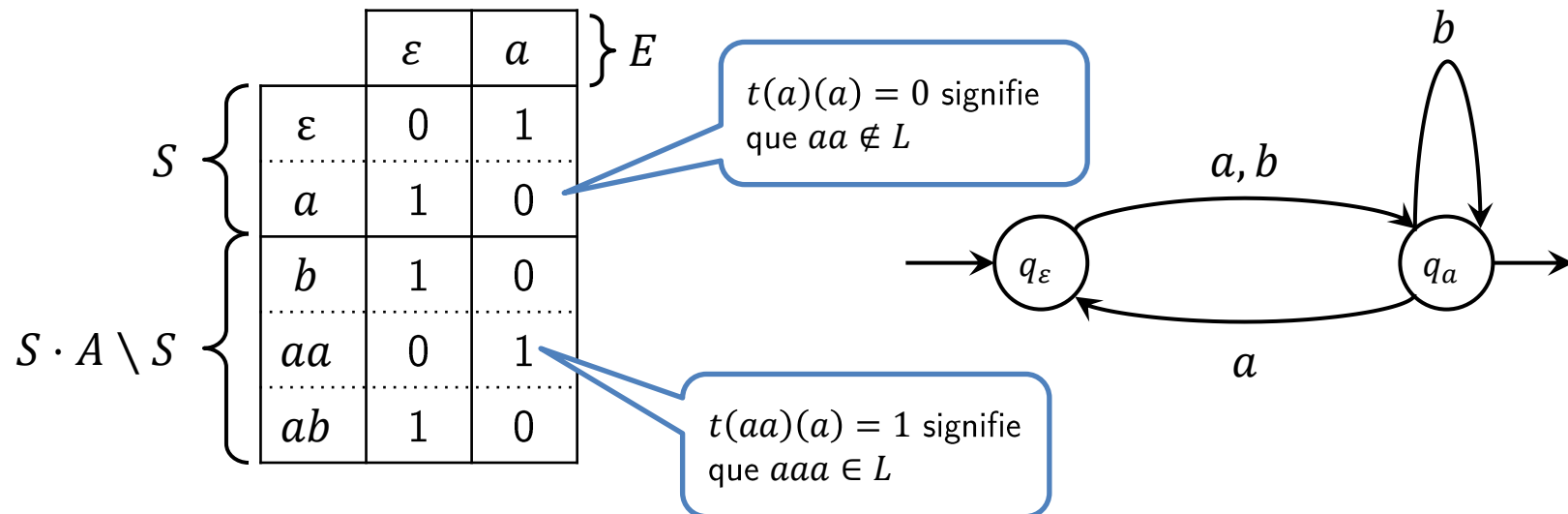
Une table d'observation est un triplet $\mathcal{T} = (S, E, t)$ où:

- S est un ensemble fini non vide et clos par préfixe de mots (lignes de la table)

$$\forall u, v \in A^*, \quad u \cdot v \in S \Rightarrow u \in S.$$
- E est un ensemble fini non vide et clos par suffixe de mots (colonnes de la table)

$$\forall u, v \in A^*, \quad u \cdot v \in E \Rightarrow v \in E.$$
- $t : (S \cup S \cdot A) \times E \rightarrow \{0,1\}$ est une fonction indiquant pour chaque ligne u et chaque colonne v si le mot $u \cdot v$ appartient au langage L .

$$\forall u \in S \cup (S \cdot A), \forall v \in E, \quad t(u)(v) = 1 \Leftrightarrow u \cdot v \in L.$$



Propriétés des tables d'observation

Table fermée : $\forall u \in S, \forall a \in A, \exists v \in S : t(u \cdot a) = t(v)$

Table cohérente : $\forall u, v \in S, t(u) = t(v) \Rightarrow \forall a \in A, t(u \cdot a) = t(v \cdot a)$

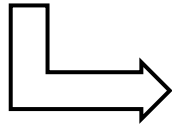
Propriété

Si $\mathcal{T} = (S, E, t)$ est fermée et cohérente, alors on peut construire un automate déterministe minimal $\mathcal{A}_{\mathcal{T}} = (Q, A, q_0, \delta, F)$ tel que:

- $Q = \{t(u) | u \in S\}$
- $q_0 = t(\varepsilon)$
- $\forall u \in S, \forall a \in A, \delta(t(u), a) = t(u \cdot a)$
- $F = \{t(u) | t(u)(\varepsilon) = 1\}$
- $\forall u \in S, \forall v \in E, u \cdot v \in \llbracket \mathcal{A} \rrbracket \Leftrightarrow t(u)(v) = 1$

Fermeture : ajouter des lignes

La table n'est pas fermée : $t(ab) \notin \{t(\varepsilon), t(a)\}$



1. Faire passer ab dans S (la partie supérieure de la table)

2. Compléter la partie inférieure de la table avec des requêtes d'appartenance.

	ε	a
ε	0	1
a	1	0
b	1	0
aa	0	1
ab	1	1

$abaa \in L?$
 $abba \in L?$
 $abba \in L?$

	ε	a
ε	0	1
a	1	0
ab	1	1
b	1	0
aa	0	1
aba	1	?
abb	?	?

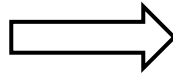
Formellement :

table non fermée ssi $\exists u, a$ tels que $t(u \cdot a) \notin \{t(v) | v \in S\}$
 $\rightarrow S := S \cup \{ua\}$

Cohérence : ajouter des colonnes

La table n'est pas cohérente: $t(a) = t(ab)$ mais $t(a \cdot a) \neq t(ab \cdot a)$

	ε	a
ε	0	1
a	1	0
ab	1	0
b	1	0
aa	0	1
aba	0	0
abb	1	0



1. Ajouter aa dans E
(l'ensemble des colonnes)
2. Compléter la table avec
des requêtes d'appartenance.

$baa \in L?$
 $aaaa \in L?$
 $abaaa \in L?$
 $abbaa \in L?$

	ε	a	aa
ε	0	1	0
a	1	0	1
ab	1	0	0
b	1	0	?
aa	0	1	?
aba	0	0	?
abb	1	0	?

Formellement :

table non cohérente ssi $\exists u, v \in S, \exists a \in A, \exists e \in E$ tels que

$$t(u) = t(v)$$

$$t(u \cdot a)(e) \neq t(v \cdot a)(e)$$

$\rightarrow E := E \cup \{a \cdot e\}$

Éléments de preuve de la propriété:

Si $\mathcal{T} = (S, E, t)$ est fermée et cohérente, alors on peut construire $\mathcal{A}_{\mathcal{T}} = (Q, A, q_0, \delta, F)$ tel que:

- $Q = \{t(u) | u \in S\}$
- $q_0 = t(\varepsilon)$
- $\forall u \in S, \forall a \in A, \delta(t(u), a) = t(u \cdot a)$
- $F = \{t(u) | t(u)(\varepsilon) = 1\}$
- $\forall u \in S, \forall v \in E, u \cdot v \in \llbracket \mathcal{A} \rrbracket \Leftrightarrow t(u)(v) = 1$

1. On commence par vérifier que $\mathcal{A}_{\mathcal{T}}$ est bien défini:

- S étant fini, Q est fini.
- Comme S est non vide, il existe un mot $s \in S$. Comme $s = \varepsilon s$, et comme S est clos par préfixe, on a $\varepsilon \in S$, soit $q_0 \in Q$.
- Soient u et v dans S tels que $t(u) = t(v)$.

Par cohérence de la table on a $t(ua) = t(va)$.

De plus, par fermeture de \mathcal{T} il existe $w \in S$ tel que $t(w) = t(ua) = t(va)$.

On vérifie donc que $\delta(t(u), a) = \delta(t(v), a) \in Q$.

2. Soit $u \in S$, on observe la propriété suivante:

$$t(u) \in F = \{t(v) | t(v)(\varepsilon) = 1\} \Leftrightarrow \exists v \in S : t(u) = t(v) \text{ et } t(v)(\varepsilon) = 1 \\ \Leftrightarrow t(u)(\varepsilon) = 1$$

Éléments de preuve de la propriété:

Si $\mathcal{T} = (S, E, t)$ est fermée et cohérente, alors on peut construire $\mathcal{A}_{\mathcal{T}} = (Q, A, q_0, \delta, F)$ tel que:

- $Q = \{t(u) \mid u \in S\}$
- $q_0 = t(\varepsilon)$
- $\forall u \in S, \forall a \in A, \delta(t(u), a) = t(u \cdot a)$
- $F = \{t(u) \mid t(u)(\varepsilon) = 1\}$
- $\forall u \in S, \forall v \in E, u \cdot v \in \llbracket \mathcal{A} \rrbracket \Leftrightarrow t(u)(v) = 1$

3. On montre que $\forall u \in S, \delta^*(q_0, u) = t(u)$ par induction sur u :

- $\delta^*(q_0, \varepsilon) = q_0 = t(\varepsilon)$
- Supposons $ua \in S$.

Comme $ua \in S$, et S est clos par préfixe, on sait que $u \in S$. Par hypothèse d'induction, on a $\delta^*(q_0, u) = t(u)$. Donc:

$$\delta^*(q_0, ua) = \delta(\delta^*(q_0, u), a) = \delta(t(u), a) = t(ua).$$

Éléments de preuve de la propriété:

Si $\mathcal{T} = (S, E, t)$ est fermée et cohérente, alors on peut construire $\mathcal{A}_{\mathcal{T}} = (Q, A, q_0, \delta, F)$ tel que:

- $Q = \{t(u) | u \in S\}$
- $q_0 = t(\varepsilon)$
- $\forall u \in S, \forall a \in A, \delta(t(u), a) = t(u \cdot a)$
- $F = \{t(u) | t(u)(\varepsilon) = 1\}$
- $\forall u \in S, \forall v \in E, u \cdot v \in \llbracket \mathcal{A} \rrbracket \Leftrightarrow t(u)(v) = 1$

4. On montre par induction sur v que $\forall v \in E, \forall u \in S, uv \in \llbracket \mathcal{A}_{\mathcal{T}} \rrbracket \Leftrightarrow t(u)(v) = 1$:

- Soit $u \in S : u\varepsilon \in \llbracket \mathcal{A}_{\mathcal{T}} \rrbracket \Leftrightarrow \delta^*(q_0, u) \in F \Leftrightarrow t(u) \in F \Leftrightarrow t(u)(\varepsilon) = 1$
- Supposons $av \in E$ et $u \in S$.

$$uav \in \llbracket \mathcal{A}_{\mathcal{T}} \rrbracket \Leftrightarrow \delta^*(q_0, uav) \in F$$

$$\text{Remarquons que } \delta^*(q_0, uav) = \delta^*(\delta(\delta^*(q_0, u), a), v) = \delta^*(t(ua), v).$$

Par fermeture de \mathcal{T} , il existe $w \in S : t(w) = t(ua)$, soit:

$$\delta^*(q_0, uav) = \delta^*(t(ua), v) = \delta^*(t(w), v) = \dots = \delta^*(q_0, wv)$$

$$\text{Donc : } uav \in \llbracket \mathcal{A}_{\mathcal{T}} \rrbracket \Leftrightarrow \delta^*(q_0, uav) \in F \Leftrightarrow \delta^*(q_0, wv) \in F \Leftrightarrow wv \in \llbracket \mathcal{A}_{\mathcal{T}} \rrbracket$$

Comme E est clos par suffixe, on sait que $v \in E$, donc par hypothèse d'induction: $wv \in \llbracket \mathcal{A}_{\mathcal{T}} \rrbracket \Leftrightarrow t(w)(v) = 1$.

$$\text{Donc : } uav \in \llbracket \mathcal{A}_{\mathcal{T}} \rrbracket \Leftrightarrow wv \in \llbracket \mathcal{A}_{\mathcal{T}} \rrbracket \Leftrightarrow t(w)(v) = 1.$$

Comme de plus $t(w) = t(ua)$ on a $t(w)(v) = t(ua)(v)$.

Enfin, remarquons que $t(ua)(v) = 1 \Leftrightarrow uav \in L \Leftrightarrow t(u)(av) \in L$.

Algorithme L^*

Membership Query:
 $MQ(u) = 1 \Leftrightarrow u \in L$

1. Initialisation : $S := \{\varepsilon\}$ et $E := \{\varepsilon\}$
2. Pour chaque $u \in S, e \in E : t(u)(e) := MQ(u \cdot e)$
3. Pour chaque $u \in S, a \in A, e \in E : t(u \cdot a)(e) := MQ(u \cdot a \cdot e)$
4. Si il existe $u, v \in S, a \in A, e \in E$ tels que $t(u) = t(v)$ et $t(ua)(e) \neq t(va)(e)$:
 - a) $E := E \cup \text{suffixes}(ae)$
 - b) Aller à l'étape 2.
5. Si il existe $u \in S, a \in A$ tels que $t(u \cdot a) \notin \{t(v) | v \in S\}$:
 - a) $S := S \cup \text{prefixes}(ua)$
 - b) Aller à l'étape 2.
6. Envoyer la requête $EQ(\mathcal{A}_{\mathcal{T}})$
7. Si l'enseignant fournit un contre-exemple u :
 - a) $S := S \cup \text{prefixes}(u)$
 - b) Aller à l'étape 2.
8. Sinon : retourner $\mathcal{A}_{\mathcal{T}}$

Equivalence Query:
 $EQ(\mathcal{A}) = ok \Leftrightarrow \llbracket \mathcal{A} \rrbracket = L$
 $EQ(\mathcal{A}) = u \Leftrightarrow \begin{cases} \text{soit } u \in L \text{ et } u \notin \llbracket \mathcal{A} \rrbracket \\ \text{soit } u \notin L \text{ et } u \in \llbracket \mathcal{A} \rrbracket \end{cases}$

Exercices

1. Montrer que le langage $L_3 := \{u \in \{a, b\}^* \mid |u|_a = |u|_b\}$ n'est pas rationnel.
2. Calculer les classes d'équivalence de \equiv_{L_4} , pour $L_4 := \{au \mid u \in \{a, b\}^*\}$.
3. Devinez mon langage secret.

Exercices – correction exo 1

1. Montrer que le langage $L_3 := \{u \in \{a, b\}^* \mid |u|_a = |u|_b\}$ n'est pas rationnel.

Considérons la suite $(a^n)_{n \in \mathbb{N}}$.

Pour toute paire $n \neq m$, on peut montrer que $a^n \not\equiv_{L_3} a^m$. En effet, en choisissant le suffixe $w := b^n$, on obtient

- $|a^n b^n|_a = n = |a^n b^n|_b$, soit $a^n b^n \in L_3$
- et $|a^m b^n|_a = m \neq n = |a^m b^n|_b$, soit $a^m b^n \notin L_3$.

En conséquence, il est impossible que deux éléments distincts de cette suite infinie appartiennent à la même classe d'équivalence.

On en déduit que la relation \equiv_{L_3} a un nombre infini de classes d'équivalence.

Autrement dit \equiv_{L_3} est **d'index infini**.

En vertu du théorème de Myhill-Nerode, cela signifie que L_3 n'est pas rationnel.

Exercices – correction exo 2

2. Calculer les classes d'équivalence de \equiv_{L_4} , pour $L_4 := \{au \mid u \in \{a, b\}^*\}$.

On va utiliser le fait que tout mot est soit vide, soit commence par un a , soit commence par un b , c'est-à-dire :

$$\boxed{\{a, b\}^* = \{\varepsilon\} \cup L_4 \cup \{bu \mid u \in \{a, b\}^*\}}.$$

- On montre que $[\varepsilon]_{L_4} = \{\varepsilon\}$:
 - $\varepsilon \equiv_{L_4} \varepsilon$: ok
 - $\varepsilon \equiv_{L_4} au \Leftrightarrow (\forall w \in \{a, b\}^*, w \in L_4 \Leftrightarrow auw \in L_4)$: impossible, car avec $w := b$, on a $b \notin L_4$ et $aub \in L_4$.
 - $\varepsilon \equiv_{L_4} bu \Leftrightarrow (\forall w \in \{a, b\}^*, w \in L_4 \Leftrightarrow buw \in L_4)$: impossible, car avec $w := a$, on a $a \in L_4$ et $bua \notin L_4$.
- On montre que $[a]_{L_4} = L_4$:
 - $a \equiv_{L_4} \varepsilon$: impossible, comme on vient de le montrer ci-dessus (contre-exemple : $w := b$).
 - $a \equiv_{L_4} au \Leftrightarrow (\forall w \in \{a, b\}^*, aw \in L_4 \Leftrightarrow auw \in L_4)$: toujours vrai, car on a $aw \in L_4$ et $auw \in L_4$.
 - $a \equiv_{L_4} bu \Leftrightarrow (\forall w \in \{a, b\}^*, aw \in L_4 \Leftrightarrow buw \in L_4)$: impossible, car on a $aw \in L_4$ et $buw \notin L_4$.
- On montre que $[b]_{L_4} = \{bu \mid u \in \{a, b\}^*\}$:
 - $b \equiv_{L_4} \varepsilon$: impossible, comme on vient de le montrer ci-dessus (contre-exemple : $w := a$)
 - $b \equiv_{L_4} au$: impossible avec ce qu'on a montré plus tôt, car $b \not\equiv_{L_4} a \equiv_{L_4} au$.
 - $b \equiv_{L_4} bu \Leftrightarrow (\forall w \in \{a, b\}^*, bw \in L_4 \Leftrightarrow buw \in L_4)$: toujours vrai, car on a $bw \notin L_4$ et $buw \notin L_4$.

On peut conclure:

$$\boxed{\{a, b\}^* = [\varepsilon]_{L_4} \cup [a]_{L_4} \cup [b]_{L_4}}$$

Exercices : correction langage secret

3. Devinez mon langage secret.

Initialement, $S = E = \{\varepsilon\}$

	ε
ε	0

On complète la partie basse :

	ε
ε	0
a	1
b	0

On observe un défaut de fermeture :

	ε
ε	0
a	1
b	0

Exercices : correction langage secret (suite)

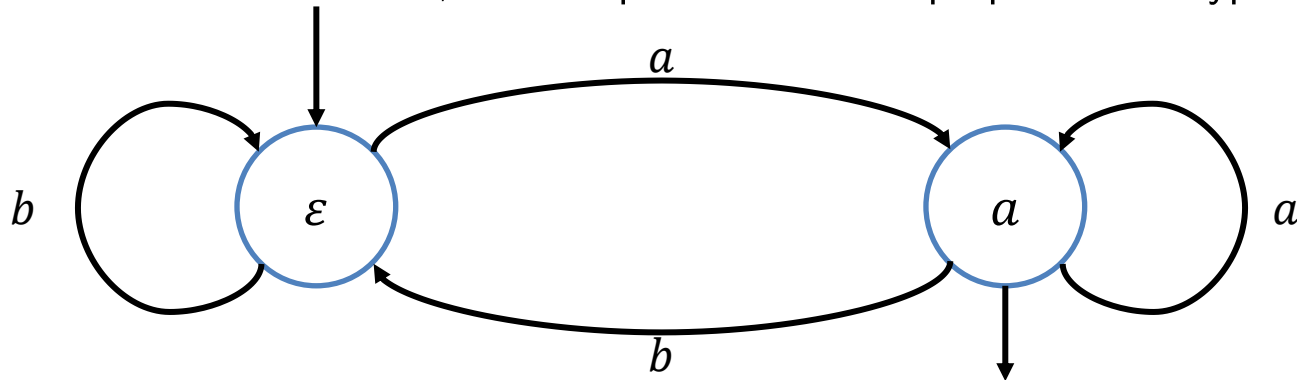
On corrige ce défaut :

	ε
ε	0
a	1
b	0

Puis on complète la partie basse:

	ε
ε	0
a	1
b	0
aa	1
ab	0

La table est fermée et cohérente, et nous permet donc de proposer une hypothèse:



L'enseignant idoine répond par le contre-exemple \boxed{aaab}

Exercices : correction langage secret (suite)

On ajoute à la partie haute le contre exemple $aaab$, ainsi que ses préfixes a, aa, aaa , puis on complète la partie basse:

	ε
ε	0
a	1
aa	1
aaa	1
$aaab$	1
b	0
ab	0
aab	0
$aaaa$	1
$aaaba$	1
$aaabb$	0

Exercices : correction langage secret (suite)

On observe un défaut de cohérence.

On le corrige en ajoutant une colonne b :

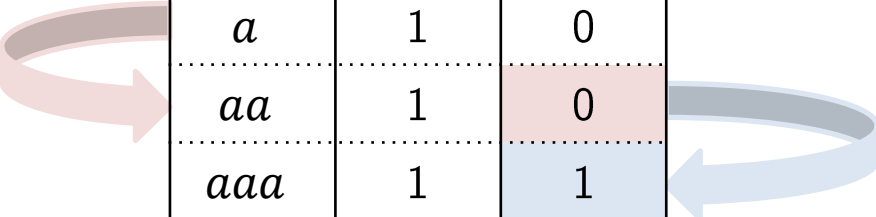
	ε
ε	0
a	1
aa	1
aaa	1
$aaab$	1
b	0
ab	0
aab	0
$aaaa$	1
$aaaba$	1
$aaabb$	0

	ε	b
ε	0	0
a	1	0
aa	1	0
aaa	1	1
$aaab$	1	0
b	0	0
ab	0	0
aab	0	0
$aaaa$	1	0
$aaaba$	1	1
$aaabb$	0	0

Exercices : correction langage secret (suite)

On observe un défaut de cohérence.

On le corrige en ajoutant une colonne ab :



	ε	b
ε	0	0
a	1	0
aa	1	0
aaa	1	1
$aaab$	1	0
b	0	0
ab	0	0
aab	0	0
$aaaa$	1	0
$aaaba$	1	1
$aaabb$	0	0

	ε	b	ab
ε	0	0	0
a	1	0	0
aa	1	0	1
aaa	1	1	0
$aaab$	1	0	1
b	0	0	0
ab	0	0	0
aab	0	0	0
$aaaa$	1	0	0
$aaaba$	1	1	0
$aaabb$	0	0	0

Exercices : correction langage secret (suite)

La table est maintenant cohérente et fermée. On remarque que dans la partie haute, les lignes aa et $aaab$ sont identiques. On peut donc simplifier la table en supprimant $aaab$ dans la partie haute.

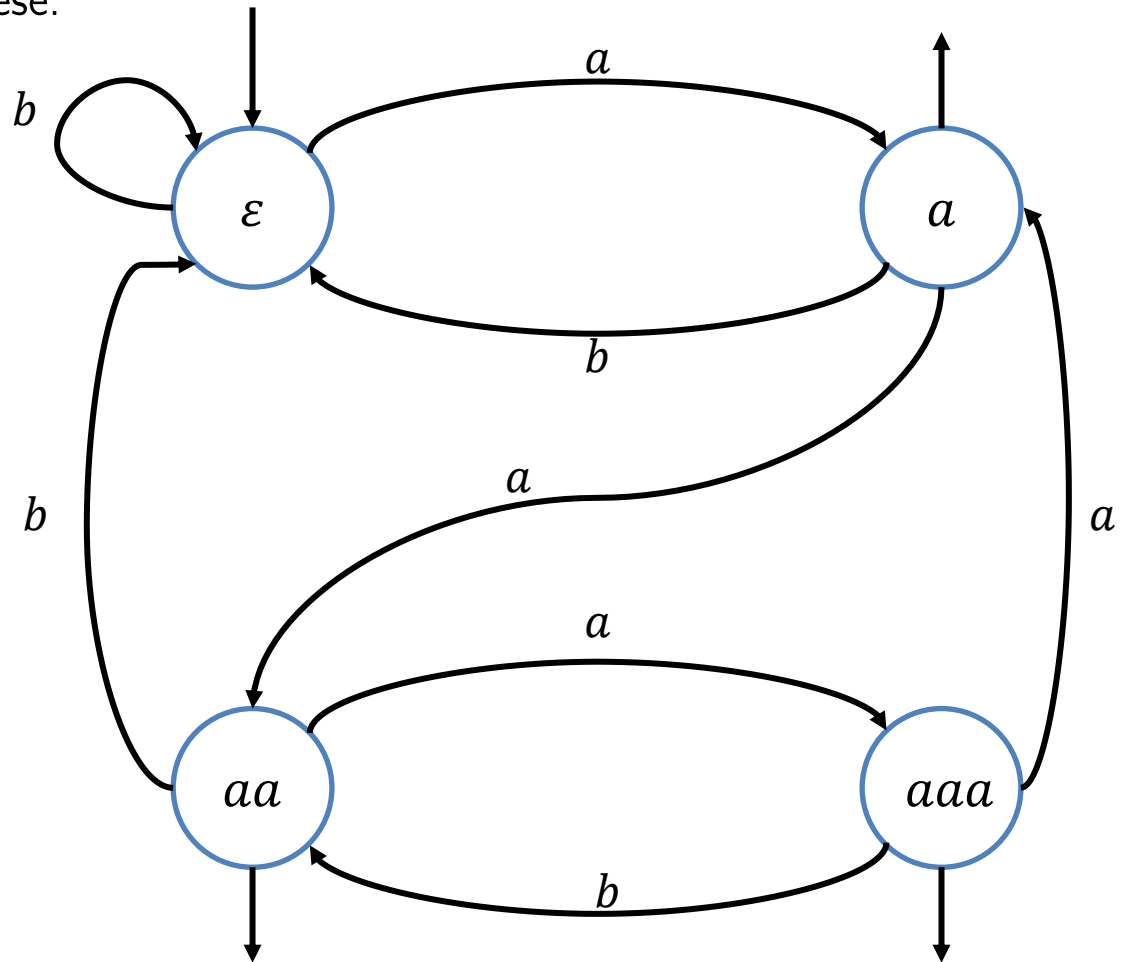
	ε	b	ab
ε	0	0	0
a	1	0	0
aa	1	0	1
aaa	1	1	0
$aaab$	1	0	1
b	0	0	0
ab	0	0	0
aab	0	0	0
$aaaa$	1	0	0
$aaaba$	1	1	0
$aaabb$	0	0	0

	ε	b	ab
ε	0	0	0
a	1	0	0
aa	1	0	1
aaa	1	1	0
b	0	0	0
ab	0	0	0
aab	0	0	0
$aaaa$	1	0	0
$aaab$	1	0	1

Exercices : correction langage secret (suite)

On construit un automate hypothèse.

	ε	b	ab
ε	0	0	0
a	1	0	0
aa	1	0	1
aaa	1	1	0
b	0	0	0
ab	0	0	0
aab	0	0	0
$aaaa$	1	0	0
$aaab$	1	0	1



L'enseignant idoine répond par le contre-exemple $baaab$.

Exercices : correction langage secret (suite)

On ajoute le contre exemple $baaab$, ainsi que ses préfixes $b, ba, baa, baaa$ à la partie haute. Ensuite on complète la partie basse.

	ε	b	ab
ε	0	0	0
a	1	0	0
aa	1	0	1
aaa	1	1	0
b	0	0	0
ba	1	0	0
baa	1	0	0
$baaa$	1	0	0
$baaab$	0	0	0
ab	0	0	0
aab	0	0	0
$aaab$	1	0	1
$aaaa$	1	0	0
bb	0	0	0
bab	0	0	0
$baab$	0	0	0
$baaaa$	1	0	0
$baaaba$	1	0	0
$baaabbb$	0	0	0

Exercices : correction langage secret (suite)

On trouve un défaut de cohérence, que l'on corrige avec la colonne *aab*.



	ε	<i>b</i>	<i>ab</i>
ε	0	0	0
<i>a</i>	1	0	0
<i>aa</i>	1	0	1
<i>aaa</i>	1	1	0
<i>b</i>	0	0	0
<i>ba</i>	1	0	0
<i>baa</i>	1	0	0
<i>baaa</i>	1	0	0
<i>baaab</i>	0	0	0
<i>ab</i>	0	0	0
<i>aab</i>	0	0	0
<i>aaab</i>	1	0	1
<i>aaaa</i>	1	0	0
<i>bb</i>	0	0	0
<i>bab</i>	0	0	0
<i>baab</i>	0	0	0
<i>baaaa</i>	1	0	0
<i>baaaba</i>	1	0	0
<i>baaabbb</i>	0	0	0



	ε	<i>b</i>	<i>ab</i>	<i>aab</i>
ε	0	0	0	0
<i>a</i>	1	0	0	1
<i>aa</i>	1	0	1	0
<i>aaa</i>	1	1	0	0
<i>b</i>	0	0	0	0
<i>ba</i>	1	0	0	0
<i>baa</i>	1	0	0	0
<i>baaa</i>	1	0	0	0
<i>baaab</i>	0	0	0	0
<i>ab</i>	0	0	0	0
<i>aab</i>	0	0	0	0
<i>aaab</i>	1	0	1	0
<i>aaaa</i>	1	0	0	0
<i>bb</i>	0	0	0	0
<i>bab</i>	0	0	0	0
<i>baab</i>	0	0	0	0
<i>baaaa</i>	1	0	0	0
<i>baaaba</i>	1	0	0	0
<i>baaabbb</i>	0	0	0	0

Exercices : correction langage secret (suite)

On trouve un défaut de cohérence, que l'on corrige avec la colonne *aaab*.



	ε	<i>b</i>	<i>ab</i>	<i>aaab</i>
ε	0	0	0	0
<i>a</i>	1	0	0	1
<i>aa</i>	1	0	1	0
<i>aaa</i>	1	1	0	0
<i>b</i>	0	0	0	0
<i>ba</i>	1	0	0	0
<i>baa</i>	1	0	0	0
<i>baaa</i>	1	0	0	0
<i>baaab</i>	0	0	0	0
<i>ab</i>	0	0	0	0
<i>aab</i>	0	0	0	0
<i>aaab</i>	1	0	1	0
<i>aaaa</i>	1	0	0	0
<i>bb</i>	0	0	0	0
<i>bab</i>	0	0	0	0
<i>baab</i>	0	0	0	0
<i>baaaa</i>	1	0	0	0
<i>baaaba</i>	1	0	0	0
<i>baaab</i>	0	0	0	0



	ε	<i>b</i>	<i>ab</i>	<i>aaab</i>	<i>aaab</i>
ε	0	0	0	0	1
<i>a</i>	1	0	0	1	0
<i>aa</i>	1	0	1	0	0
<i>aaa</i>	1	1	0	0	0
<i>b</i>	0	0	0	0	0
<i>ba</i>	1	0	0	0	0
<i>baa</i>	1	0	0	0	0
<i>baaa</i>	1	0	0	0	0
<i>baaab</i>	0	0	0	0	0
<i>ab</i>	0	0	0	0	0
<i>aab</i>	0	0	0	0	0
<i>aaab</i>	1	0	1	0	0
<i>aaaa</i>	1	0	0	0	0
<i>bb</i>	0	0	0	0	0
<i>bab</i>	0	0	0	0	0
<i>baab</i>	0	0	0	0	0
<i>baaaa</i>	1	0	0	0	0
<i>baaaba</i>	1	0	0	0	0
<i>baaab</i>	0	0	0	0	0

Exercices : correction langage secret (suite)

On supprime les lignes
redundantes.

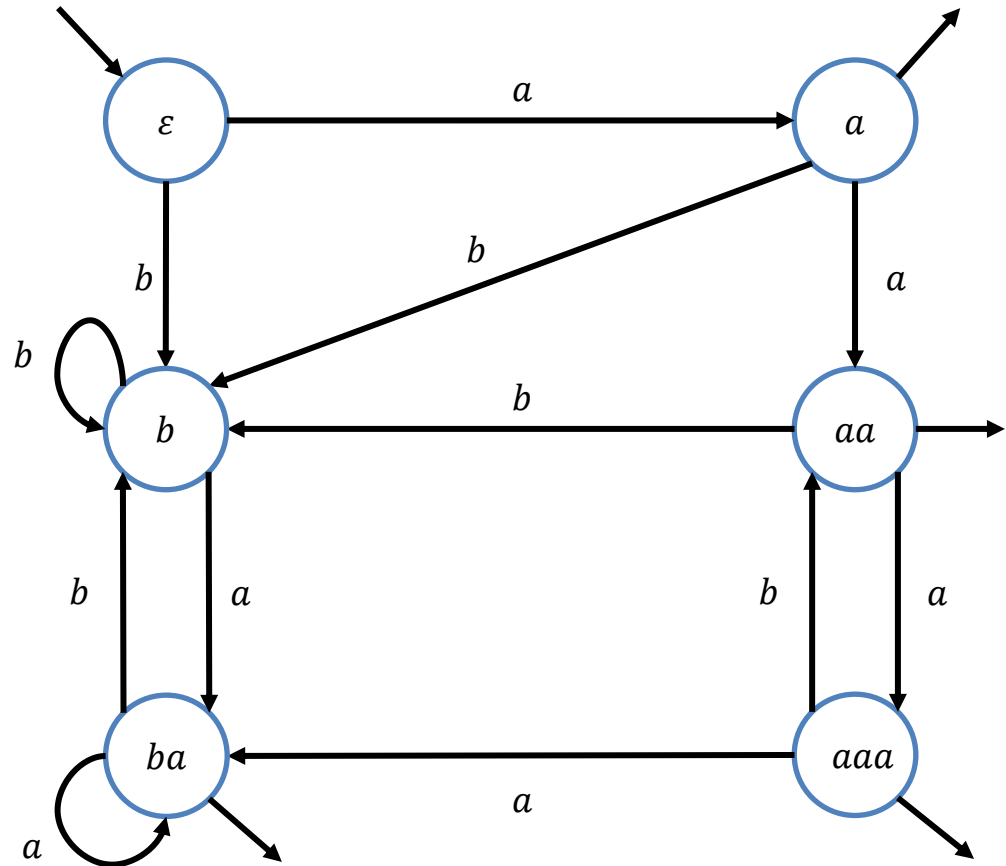
	ε	b	ab	aab	$aaab$
ε	0	0	0	0	1
a	1	0	0	1	0
aa	1	0	1	0	0
aaa	1	1	0	0	0
b	0	0	0	0	0
ba	1	0	0	0	0
baa	1	0	0	0	0
$baaa$	1	0	0	0	0
$baaab$	0	0	0	0	0
ab	0	0	0	0	0
aab	0	0	0	0	0
$aaab$	1	0	1	0	0
$aaaa$	1	0	0	0	0
bb	0	0	0	0	0
bab	0	0	0	0	0
$baab$	0	0	0	0	0
$baaaa$	1	0	0	0	0
$baaaba$	1	0	0	0	0
$baaabb$	0	0	0	0	0

	ε	b	ab	aab	$aaab$
ε	0	0	0	0	1
a	1	0	0	1	0
aa	1	0	1	0	0
aaa	1	1	0	0	0
b	0	0	0	0	0
ba	1	0	0	0	0
ab	0	0	0	0	0
aab	0	0	0	0	0
$aaab$	1	0	1	0	0
$aaaa$	1	0	0	0	0
bb	0	0	0	0	0
baa	1	0	0	0	0
bab	0	0	0	0	0

Exercices : correction langage secret (suite)

On construit l'automate hypothèse.

	ε	b	ab	aab	$aaab$
ε	0	0	0	0	1
a	1	0	0	1	0
aa	1	0	1	0	0
aaa	1	1	0	0	0
b	0	0	0	0	0
ba	1	0	0	0	0
ab	0	0	0	0	0
aab	0	0	0	0	0
$aaab$	1	0	1	0	0
$aaaa$	1	0	0	0	0
bb	0	0	0	0	0
bab	0	0	0	0	0



L'enseignant idoine répond que c'est le bon automate. Nous sommes alors heureux.

On peut aussi extraire de l'automate une expression régulière : $(a + b)^* a + aa(ab)^*$.